SANTA FE TRAIL
TECHNOLOGY DEPARTMENT

Updated: 6/24/25

USD434 Acceptable Use Policy

I. Purpose The district provides computer network and internet access for its students and employees. This service allows employees and students to share information, learn new concepts, research diverse subjects, and create and maintain school-based websites. The district has adopted the following Acceptable Use Guidelines to govern the conduct of those who elect to access the computer network or district Internet. This policy also outlines the acceptable use, maintenance, and security protocols for all computer systems and electronic devices issued by the district. Our aim is to ensure the efficient, secure, and appropriate use of district technology resources for educational and professional purposes, while also clarifying privacy expectations and user responsibilities. Before receiving a district device, all staff, students and their parent/guardian must electronically sign this policy as part of the enrollment process, signifying their understanding and agreement to adhere to these guidelines. All student devices must be returned in satisfactory condition for maintenance and summer storage at the end of each school year.

II. Scope district issued computer systems and electronic devices (including, but not limited to, Smartboards, iPads, iTouches, iPhones, eReaders, and eBooks) as well as components on the district's network and security systems. It applies to all staff and students using these resources, and to personal devices brought onto the district network by staff. While this policy specifically addresses district computer systems and electronic devices, it operates under the broader framework of Policies IIBF, IIBG, IIBGA, IIBGC, ECH, GAT, JDD, JS & KGA.

III. Users shall adhere to the following guidelines of Policy Statements & Acceptable Use Guidelines

A. **Acceptable Use, Use of District Computers and Devices & Privacy Rights**
   - District-issued computer systems and electronic devices are provided solely for educational and professional use.
   - All information created by staff or stored thereon shall be considered district property and shall be subject to unannounced monitoring by district administrators.
   - Unauthorized access to and/or unauthorized use of the district server or security system (including, but not limited to, surveillance footage) is also prohibited.
   - Employees and/or students shall have no expectation of privacy when using district e-mail or other official communication systems. Any e-mail or computer application or information in district computers, computer systems, or electronic devices is subject to monitoring by the administration.
   - All use of the Internet will be in support of educational activities.
   - Users will report misuse and breaches of network security.
   - Users shall not access, delete, copy, modify, nor forge other users' e-mails, files, or data.
   - Users shall not use other users' passwords nor disclose their password to others.
   - Users shall not pursue unauthorized access, disruptive activities, nor other actions commonly referred to as "hacking," internally or externally to the district.
   - Users shall not disclose confidential information about themselves or others.

B. **Copyright**
   - The copyright laws of the United States make it illegal for anyone to duplicate copyrighted materials without permission. Severe penalties are provided for unauthorized copying of all materials covered by the act unless the copying falls within the bounds of the "fair use" doctrine.

- ○ Any duplication of copyrighted materials by district employees must be done with permission of the copyright holder or within the bounds of "fair use."
- ○ The legal or insurance protection of the district shall not be extended to school employees who violate any provisions of the copyright laws.
- ○ Software acquired by staff, using either district or personal funds, and installed on district computers or electronic devices must comply with copyright laws.
- ○ Proof of purchase (copy or original) for software must be filed in the Technology Department.
- ○ See Policy ECH for a comprehensive guide to copyright regulations and fair use rules for educators.

C. **Software and Application Installation**

- ○ Users shall not utilize unlicensed software
- ○ No software, including freeware and shareware, or other applications may be installed on any district computer or electronic device until cleared by the Technology Director.
- ○ The Technology Director (or assignee) will verify the compatibility of the software or application with existing software, hardware, and applications, verify the security of software, and prescribe installation and de-installation procedures.
- ○ For Chromebooks and iPads, users must request app installation or use the built-in app store. Avoid downloading apps from untrusted sources.

D. **Hardware Care & Maintenance** Users are responsible for the proper care and maintenance of district-issued devices. This includes:

- ○ Users shall not install unapproved hardware on district computers or make changes to software settings that support district hardware.
- ○ Keeping it Clean: Regularly wipe the screen, keyboard, and exterior of the device with a soft, dry cloth. Avoid harsh chemicals or abrasive materials.
- ○ Handling with Care: Treat the device gently, avoiding dropping or mishandling. Use a protective case, bag or sleeve when transporting.
- ○ Power Management: Power down the device properly when not in use to ensure updates are installed and conserve battery life.
- ○ Software Updates: Allow devices to install software updates regularly. These updates include security patches, bug fixes, and performance improvements.
- ○ Storage Management: Periodically clean out unnecessary files and apps to free up local storage space and maintain performance. Utilize cloud storage options where available.
- ○ Security Awareness: Exercise caution when browsing the web and downloading files. Avoid clicking on suspicious links or downloading attachments from unknown sources.
- ○ Temperature and Environment: Keep devices in a temperate environment, away from extreme heat, cold, or high humidity. Avoid using on soft surfaces.
- ○ Battery Care: Avoid constantly draining the battery to zero or constantly charged at 100%. Aim to keep the charge between 20% and 80% for optimal battery health. For extended storage, charge the battery to approximately 50%.
- ○ Peripheral Use: Exercise caution when using or unplugging accessories such as chargers, mice, or USB drives to prevent damage to ports or other components.

E. **Audits** The administration may conduct periodic audits of software and applications installed on district equipment to verify legitimate use. These audits may be performed to ensure compliance with copyright laws, verify adherence to licensing agreements, maintain system security, or confirm appropriate use of district technology resources.

F. **Ownership of Employee Computer and Device Materials** Computer materials, devices, software, or applications created as part of any assigned district responsibility or classroom activity undertaken on school time shall be the property of the board.

G. **Lost, Stolen, or Damaged Computers and/or Equipment**
   - Students and staff members shall be responsible for reimbursing the district for replacement of or repair to district issued computers or electronic devices which are lost, stolen, or damaged while in the students' or staff members' possession.
   - The Superintendent may, at their discretion and based on certain circumstances, choose to waive this fee.
   - In cases of stolen equipment producing a police report maybe required.
   - These specific responsibilities for electronic devices align with the broader principles for personal use, lost, stolen, or damaged personal property outlined in Policy KGA.

H. **Staff & Student - Fee & Replacement Costs**
   - A $25 replacement fee will be assessed for damage or loss of the charger or case.
   - A $40 repair fee will be assessed for minor damages to the device requiring replacement parts or repair.
   - A $300 replacement fee will apply for Chromebooks, with costs for other device types to be determined, for:
     - Intentional damage making the device reasonably non-repairable.
     - Loss of the device.
     - Excessive damage.
   - Subject to the building administrator's discretion and device availability, a substitute device may be provided for use while your original device is being serviced.
   - Repayment of fees are subject to our districts JS Student Fees and Charges Policy.

I. **Bring Your Own Device (BYOD)**
   - **Staff BYOD**: Staff members are permitted to bring their own personal electronic devices (e.g., laptops, tablets, smartphones) for use on the district network. However, the district strongly discourages the use of personal devices for official district business or the storage of sensitive district data. Staff bringing personal devices do so at their own risk. The district is not responsible for the security, maintenance, or repair of personal devices, nor for any loss of data on such devices. Staff personal devices connecting to the district network must comply with all district security protocols and policies, including but not limited to acceptable use guidelines and network security requirements. Additionally, personal devices connected to WiFi will be filtered with logging enabled.
   - **Student BYOD**: Students are strictly prohibited from bringing their own personal electronic devices for use within the instructional environment or for connecting to the district network. All student technology use must be conducted on district-issued devices. This prohibition is in place to ensure a consistent and secure learning environment, protect student privacy, and manage equitable access to educational resources.

J. **Prohibited Actions** Although the district reserves the right to determine what use of the district network is appropriate, the following actions are specifically prohibited:
   - Transferring copyrighted materials to or from any district network without the express consent of the owner of the copyright.
   - Use of the network for creation, dissemination, or viewing of defamatory, factually inaccurate, abusive, obscene, profane, sexually oriented, threatening, harassing, or other material prohibited by law or district policy.

- Dissemination of personnel or student information via the network when such information is protected by law, including the Family and Educational Rights Act or Student Data Privacy Act
- Utilization of the network to disseminate non-work-related material.
- Utilization of the network as a means for advertising or solicitation.
- Users shall not access or permit access to pornography, obscene depictions, or other materials harmful to minors.
- Users shall not disable or attempt to disable Internet filtering software.

K. **Monitoring** The school district reserves the right to monitor, without prior notice, any and all usage of the computer network and district Internet access, including, but not by way of limitation, e-mail transmissions and receptions. Any information gathered during monitoring may be copied, reviewed, and stored. All such information files shall be and remain the property of the school district, and no user shall have any expectation of privacy regarding his/her use of the computer network or the district Internet.

L. **Internet Safety** In compliance with the Children's Internet Protection Act (CIPA) and the Kansas Children's Internet Protection Act, the school district will implement filtering and or blocking software to restrict access to Internet sites containing child pornography, obscene depictions, or other materials harmful to minors. The school district, however, cannot and does not guarantee the effectiveness of filtering software. Users encountering inappropriate content must take immediate action:

- Any student who connects to such a site must immediately disconnect from the site and notify a teacher
- An employee who accidentally connects to such a site must immediately disconnect from the site and notify a supervisor.
- If a user sees another user is accessing inappropriate sites, he or she should notify a teacher or supervisor immediately.

The school district administration reserves the right to prohibit access to any network or Internet it deems inappropriate or harmful. See Policy IIGBA for the districts board approved CIPA Plan.

M. **Cyberbullying Prohibition:** The district is committed to providing a safe and positive learning and working environment. Cyberbullying is strictly prohibited and will not be tolerated.

- **Definition of Cyberbullying:** Cyberbullying includes any act of bullying committed by use of electronic communication, including without limitation, any communication made by means of a computer, computer network, electronic mail, Internet-based communication, telecommunication, or wireless communication. This includes, but is not limited to, actions that:
  - Humiliate, harass, intimidate, or threaten another individual.
  - Spread rumors, gossip, or false information about another individual.
  - Share private or embarrassing information, photos, or videos of another individual without their consent.
  - Exclude or isolate another individual from online groups or activities.
  - Impersonate another individual online to cause harm or embarrassment.
  - Damage another individual's reputation, property, or well-being.
- **Expectations for Online Behavior:** The district shall provide instruction to students regarding appropriate online behavior, including recognizing, responding to, and reporting cyberbullying. All users are expected to conduct themselves respectfully and ethically in all online interactions.
- **Reporting Cyberbullying:** Users who experience cyberbullying, or who witness cyberbullying, are strongly encouraged to report it immediately to a teacher, school administrator, or supervisor. All reports will be taken seriously and investigated promptly.

N. **Penalties for Improper Use & Enforcement:** Access to the network and Internet is a privilege, not a right, and inappropriate use will result in the restriction or cancellation of the access. The school district has the right to make the determination of what constitutes inappropriate use and use as an educational tool. Inappropriate use, including engagement in cyberbullying, may lead to any disciplinary and/or legal action, up to and including suspension and/or expulsion of district students and suspension and/or termination of employees. Law enforcement shall be notified of inappropriate use which may constitute a violation of Federal or state law, and such use may result in criminal prosecution. See Policy JDD for the board approved Suspension and Expulsion Procedures.

O. **Staff Online Activities and Social Networking:** All staff online activities, especially those involving social networking and communication with students and parents, are governed by the detailed rules in Policy IIBGC.

- Employees are encouraged to use district electronic mail and other district technology resources to promote student learning and communication with parents of students and education-related entities. If those resources are used, they shall be used for purposes directly related to work-related activities. Technology-based materials, activities, and communication tools shall be appropriate for and within the range of the knowledge, understanding, age, and maturity of students with whom they are used.
- Staff, including teachers and activity sponsors, may utilize blogs and social networking accounts provided through district resources for school-related activities and supplementing instruction, but **prior permission from the superintendent or designee is required**. If granted, the site must adhere to district guidelines, including potential administrator/tech access and prior approval for any district expenditures. For student access, staff must obtain written parental consent if not already covered by the acceptable use policy.
- Sponsoring staff are responsible for monitoring and managing these sites to ensure safe, acceptable use and compliance with district policies, while strictly observing confidentiality regarding personally identifiable student information under state and federal law. The district **discourages staff from creating personal social networking accounts to which they invite current or future students to be friends**, and employees doing so assume all associated risks. All employees are expected to protect students' health, safety, emotional well-being, and confidentiality of student record information in all online actions. Violations of this policy or other applicable guidelines, including those related to technology and online resources, may result in disciplinary action up to and including termination of employment.

P. **Staff Communication Device Use:** This section relating to staff communications devices is governed by the detailed rules in Policy GAT. The board encourages district employees to use technology, including communication devices, to improve efficiency and safety. The district expects all employees to use communication devices in a responsible manner that does not interfere with the employee's job duties. Employees who violate district policies and procedures governing the use of communication devices may be disciplined, up to and including termination, and may be prohibited from possessing or using communication devices while at work. Communication devices may not be used in any manner that would violate the district's policy on student-staff relations.

- **"Communication device"** is defined to include all portable devices that send or receive calls or text messages, allow the retrieval of email, or provide access to the Internet. Communication devices shall include, but may not be limited to cell phones, smart phones, iPads, and tablets.
- **Use During Student Supervision and Instruction:** Supervision of students and the provision of academic instruction are priorities in the district, and employees who are responsible for supervising and/or providing academic instruction to students must concentrate on these tasks at all times. Employees shall not use communication devices when they are responsible for

supervising students or when their doing so interrupts or interferes with classroom instruction unless any of the following conditions occurs:

- The device is being used to instruct the students being supervised at the time
- The use is necessary to the performance of an employment-related duty
- The employee has received specific and direct permission from a supervisor to do so or
- There is an emergency.

Even when these conditions exist, the employee is responsible for obtaining assistance in adequately supervising students during the approved use so that students are supervised at all times.